A Strategic Model of Cyber-Security with Multiple Agents and Actions

Jomon A. Paul and Abhra Roy *

Preliminary Draft

Abstract

We analyze a model of cybersecurity involving multiple firms and strategic attackers. Specifically, we employ a novel location choice framework embedded in a non-cooperative game with both sequential and simultaneous elements to study the provision of cybersecurity. The location choice framework is designed to capture the firms network connectivity with the distance from the location of the firm to the boundary that they share representing the firm's network ties vertically (or a lack of segmentation with other firms in its network). The hackers attempt to hack the firms and inflict damage by choosing the 'location' of the attack (a point between the firm's location and its boundary) and the effort to be exerted. The firms devote three types of resources to counter the threat from a cyberattack, namely, prevention, detection, and containment. In this context, we capture the strategic interactions between (a) the choice of location and avoiding detection by the hacker; (b) the hacker and the firm; (c) the instruments of cyberdefense at the firms' disposal; (d) between the firms. Finally, we investigate the utility of information sharing in cybersecurity and report several novel results. We find that if the information on detection is valuable (i.e., the marginal cost of detection is higher than a certain threshold), then information sharing is beneficial (both firms increase detection and prevention). However, if the cost of detection is below a certain threshold, then information sharing makes both firms more vulnerable (both firms decrease detection and prevention). Our model also notably shows that cybersecurity under a social planner may be the best way to

*Department of Economics, Finance and Quantitative Analysis,
Kennesaw State University,
560 Parliament Garden Way, Kennesaw, Ga-30144.
Electronic address:aroy1@kennesaw.edu; jpaul17@kennesaw.edu